Violation of ISP licence by Bharati

155. SHRI N.R. GOVINDARAJAR: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government have issued showcause notice to the any private telecom operator for violating ISP licence;

(b) whether it is a fact that 13 internet leased lines subscribers of the said company are receiving international calls and also further illegally switched to various subscribers; and

(c) if so, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DR. SHAKEEL AHMAD): (a) Yes, Sir.

(b) and (c) It has been reported that 13 Internet Leased line subscribers of M/s Bharti Infotel Ltd in Bangalore and Chennai were found receiving international voice calls and further switching them illegally to various subscribers. Based on these reports, a showcause notice for imposition of penalty has been issued to M/s Bharti Infotel Ltd. under Licence Agreement for provision of Internet Service (Including Internet Telephony) for breach of terms and conditions of the Licence Agreement.

Data tampering and e-fraud

156. SHRI R.K. ANAND: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that computerization of Government functions, exposes organization to risk of data tampering and e-fraud;

(b) if so, the details thereof; and

(c) what arrangement had been made to ensure data safety?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DR. SHAKEEL AHMAD): (a) Yes, Sir.

(b) Data tampering is deliberately entering false data, or changing and deleting true data. E-fraud is illegal transaction.

(c) Computerised Application Systems performing Government functions are developed, keeping different levels of security in place, as per the requirements:

(i) Physical security for the computers storing the sensitive data is in place, as prescribed by standard govt. procedures.

(ii) Only authorized users are allowed to access the data as per the permissions granted.

(iii) Steps are taken for performing penetration tests before applications being made available to the public/users.

(iv) Critical Applications have additional authentication through digital signatures through which encruption of data during transmission/ storage takes place.

(v) The data is kept in secure zones protected using state-of-art technologies, such as, firewalls, intrusion prevention system etc. and on secured servers.

(vi) Access control measures, such as, Virtual Private Network (VPN)/ Secure Socket Layer (SSL) for authenticated and secure content updation are in place.

(vii) Latest security patches for the vulnerabilities on the system and application software and applied.

(viii) Through regular application security audit and Operating System (OS) hardening procedures, the application code, the associated procedures and policies and the functional controls are checked.

Thus all possible steps are being taken to minimise the possibility of tempering and e-fraud of data on computerized systems.

Purchase of SIM cards by naxalites

157. SHRI DATTA MEGHE: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it has come to the notice of the Government that naxalites have procured 400 SIM cards from Bharat Sanchar Nigam Limited (BSNL);

(b) if so, the details thereof;